HOWARD COUNTY BRAC TASK FORCE
BRAC BIT: # 79
DATE: 27 May 2010
SUBJECT(S): Cyber Article
POINT OF CONTACT: Kent Menser (410-313-6521) kmenser@howardcountymd.gov

By LOLITA C. BALDOR (AP) OMAHA, Neb. — A U.S. government computer security system that can detect and prevent cyber attacks should be extended to private businesses that operate critical utilities and financial services, a top Pentagon official said Wednesday.

"William J. Lynn III, the deputy defense secretary, said discussions are in the very early stages and participation in the program would be voluntary. The idea, he said, would allow businesses to take advantage of the Einstein 2 and Einstein 3 defensive technologies that are being developed to put in place on government computer networks.

Extending the program to the private sector raises a myriad of legal, policy and privacy questions, including how it would work and what information — if any — companies would share with the government about any attacks or intrusions they detect.

Businesses that opt not the participate could "stay in the wild, wild west of the unprotected Internet," Lynn told a small group of reporters during a cybersecurity conference.

And in the case of Einstein 2 — an automated system that monitors federal Internet and e-mail traffic for malicious activity — companies already may have equal or superior protections on their networks.

"Einstein 2 is like a 1999 Mustang with a little rust," said James Lewis, a cybersecurity expert and senior fellow at the Washington-based Center for Strategic and International Studies. "For some companies it isn't a big deal. But for others who haven't done much (to secure their networks) it would be a good idea."

Lewis said the larger challenges would come with Einstein 3, a separate program being developed which would detect and actively block or prevent cyber intrusions.

Einstein 2 is in place in at least 11 of the 21 government agencies that police their own networks. The other 89 federal agencies will go through one of four major technology contractors for the Einstein monitoring. Einstein 3 is currently in a trial phase.

Managed and run by the Homeland Security Department, the two systems have triggered debate over whether they violate privacy. But the Justice Department concluded last year that it doesn't violate the rights of either the federal employees or the private citizens who communicate with them.

According to Lewis, there are questions about whether companies would share with the government information they collected on malicious Internet traffic. At the same time, the government would find it difficult to share some threat assessment information with industry because it may be classified. And companies might hesitate to share data with each other due to competitive concerns.

One Homeland Security official said the department and the Pentagon are working together to secure government networks, and are relying on private sector and government technical expertise to do that.

That experience will provide insight into ways to protect the privately owned and operated critical infrastructure, said the official, who spoke on condition of anonymity because discussions are in early stages.

Lynn and Air Force Gen. Kevin Chilton, commander of U.S. Strategic Command, on Wednesday also warned of escalating threats from cyber espionage and computer crimes. They called for more cooperation between the federal government and private industry, as well as between nations.

The Pentagon's creation of U.S. Cyber Command, which officially launched on Friday, will help the Defense Department protect its networks and enable it to better assist other federal agencies when they are hit with a cyber attack, Chilton said.

But he acknowledged it will be challenging to develop rules of cyber warfare, including what constitutes a cyber attack and what is an appropriate response. The new Cyber Command will be based at Fort Meade, Md., and it will report to the Strategic Command in Omaha.

U.S. computer networks face persistent attacks, including complex criminal schemes, suspected cyber espionage by other nations such as China, and possible terrorist probes seeking vulnerable systems or sensitive information.

Critics long have complained that defense officials have not yet detailed how and when the U.S. military should conduct cyber warfare, and what constitutes a computer-based attack that requires retaliation."